AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: /S Bow Bottomly 03/12/2024

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of
(Briefly describe the property to be search
Or identify the person by name and address)
PROPERTY KNOWN AS:
Apple iPhone 13 Pro Max, SN: RQWHJXMTPH

IN POSSESSION OF:
Army Criminal investigation Division
2635 Miner Rd.
Fort Sill, OK, 73503

Case No: M-24- 223-AMG

APPLICATION FOR SEARCH WARRANT

I, James D. Hawkins, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property *(identify the person or describe property to be searched and give its location)*:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252 and 2252A	Distribution of child pornography
18 U.S.C. §§ 2252 and 2252A	Receipt of child pornography
18 U.S.C. §§ 2252 and 2252A	Possession of child pornography

The application is based on these facts:

See attached Affidavit of Special Agent James D. Hawkins, Armey Criminal Investigation Division (Army CID), which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

James D. Hawkins
Special Agent
Army CID

Sworn to before me and signed in my presence.

Date: 3/12/2024

City and State: Oklahoma City, Oklahoma

Judge's signature

AMANDA MAXFIELD GREEN, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, James D. Hawkins, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant to search for and seize evidence of Title 18 of the United States Code Sections 2252 and 2252A (possession, receipt, and distribution of child pornography)located within one (1) Apple iPhone 13 Pro Max, serial number RQWHJXMTPH, currently in law enforcement possession at the Criminal Investigation Division, 2635 Miner Rd. Fort Sill, OK 73503. The cell phone to be searched are described in the following paragraphs and in Attachment A.

2. I am a Special Agent of The Department of the Army Criminal Investigation Division and have been since November 2008. I have been designated by a law as a Federal Law Enforcement Officer, authorized to received and serve federal and civilian search warrants and authorizations. As a Special Agent, I received training in the process and procedures of investigating felony level crimes at the Criminal Investigation Division Special Agent Course. Additionally, I have received training in crime processing, and the procedures and practices associated with the collection of physical and testimonial evidence. As a Special Agent, I am empowered to investigate violation of the Uniformed Code of Military Justice and applicable Federal and State laws where there is an Army interest. This affidavit is intended to show merely there is sufficient probable cause for the requested search authorization. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of Title 18, United States Code, Sections 2251, 2252, and 2252A. I have received training and instruction in the field of investigation of child pornography and have had

the opportunity to participate in investigations relating to the sexual exploitation of children. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as digital storage devices, the Internet, and printed images).

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from my review of local law enforcement reports and interviews of witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience, evidence of criminal activity, to include motives, operational planning, operational preparation, and other relevant evidence will be found in the criminal's electronic devices including their cell phone. This evidence often includes location data stored in the internal memory of the cell phone, encrypted communications between co-conspirators, non-encrypted communications between co-conspirators in the form of emails and text messages, and other accounts linked to the criminal and their criminal activity to include social media accounts which can be used in the planning and execution of a crime.

5. Based on the information set forth below, there is probable cause to believe that this wireless phone, seized from the subject of my investigation, identified as one (1) Apple iPhone 13 Pro Max serial number RQWHJXMTPH, and hereinafter referred to as "The DEVICE" and any and all evidence referenced in Attachment B, is related to violations of Title 18 of the United States Code Sections 2252 and 2252A (possession, receipt, and distribution of child pornography). There is probable cause to believe that a search of the DEVICE will lead to evidence, fruits, and instrumentalities of the aforementioned crimes.

6. This court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. §§ 2711, 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States. . . that has jurisdiction over the offense being investigated" 18 U.S.C. §2711(3)(A)(i), and "is in . . . a district in which the provider . . . is located or in which the wire or electronic communication, records, or other information are stored." 18 U.S.C. §2711(3)(A)(ii).

TECHNICAL TERMS AND DEFINITION

7. Based on my training and experience, I use the following technical terms to convey the following meanings and apply to this Affidavit and Attachment B:

a. A "wireless telephone" (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. A "GPS" navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

c. An "Internet Protocol address" (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

e. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

f. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

g. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C), which includes as any visual depiction of sexually explicit conduct involving the use of a minor; a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaged in sexually explicit conduct; or a visual depiction that has been created, adapted, or modified to appear than an identifiable minor is engaging in sexually explicit conduct. In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether

between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

h. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

PROBABLE CAUSE

8. The National Center for Missing and Exploited Children ("NCMEC") is an organization that, among other things, tracks missing and exploited children, and serves as a repository for information about child pornography. Companies that suspect child pornography has been stored or transmitted on their systems can report that information to NCMEC in a cybertip. To make such a report, a company providing services on the internet ("ISP") can go to an online portal that NCMEC has set up for the submission of these tips. The ISP then can provide to NCMEC information about the child exploitation activity it believes has occurred, including the incident type, the incident time, any screen, or usernames associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. Other than the incident type and incident time, the remainder of the information the ISP provides is voluntary and undertaken at the initiative of the reporting ISP. The ISP may also upload to NCMEC any files it collected in connection with the activity. The ISP may or may not independently view the content of the files it uploads. NCMEC does not review the content of these uploaded files. Using publicly available search tools,

NCMEC then attempts to locate where the activity occurred based on the information the ISP provides such as IP addresses. NCMEC then packages the information from the ISP along with any additional information it has, such as previous related cybertips, and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

9. On June 21, 2023, Dropbox (ISP) submitted a Cybertipline Report # 164819507 to the National Center for Missing and Exploited Children ("NCMEC"). The incident type was: Child Pornography (possession, manufacture, and distribution), and the incident time was listed as: June 20. 2023. The ISP also uploaded file(s) in connection with the report, the content of which NCMEC did not review. The report did indicate that the ISP reviewed the contents of the file(s). The ISP reported the following additional information; IP address: 74.195.178.116, email address: Kris.purple26@gmail.com, screen username: Kristian Fernandez, and ESP ID: 569824786.

10. NCMEC then used publicly available search tools to discover that the IP address the ISP reported resolved to an address in Los Angeles, California.

11. I know the ISP flag and reports images or files that have the same "hash values" as images that have been reviewed and identified by NCMEC or by law enforcement as child pornography. A hash value is akin to a fingerprint for a file. The contents of a file are processed through a cryptographic algorithm, and a unique numerical value is produced that identifies the unique contents of the file. If the contents are modified in any way, the value of the hash will also change significantly. I know that the chances of two files with different content having the same hash value are extremely small.

12. I know the ISP compares the hash values of files that its customers transmit on its systems against the list of hash values that NCMEC has. If the ISP finds that a hash value of a file

on its systems matches one on the list, it captures the file along with information about the user who posted, possessed, or transmitted it on the ISP's systems.

13. I also know that the ISP uses PhotoDNA. PhotoDNA is a software technology developed by Microsoft that computes hash values of images, video and audio files to identify alike images. PhotoDNA is primarily used in the prevention of child pornography proliferation. Here, that technology was used to determine that a user of its services posted or transmitted a file with the same hash value as an image that has previously identified as containing child pornography.

14. On February 5, 2024, a DACID agent reviewed the files provided with Cybertipline Report # 164819507 and confirmed the downloaded files contained Child Sexual Abuse Material (CSAM) a/k/a child pornography.

15. On February 15, 2024, DACID agents interviewed PV2 Kristian FERNANDEZ. PV2 FERNANDEZ was read his *Miranda* rights, waived his rights, and agreed to be interviewed. PV2 FERNANDEZ stated he received, possessed, and viewed CSAM with the intent of downloading such images and videos to distribute in a group chat called "Reddit against degenerative subs" on the Reddit application on his Apple iPhone 13 Pro Max, serial number RQWHJXMTPH. PV2 FERNANDEZ stated he clicked on the links provided during his search for CSAM, download the images/videos, and attached them to a message in the chat group "Reddit against degenerative subs." PV2 FERNANDEZ stated his intent in doing this was reporting such web links to people within "Reddit against degenerative subs" group. PV2 FERNANDEZ stated he did not use any other devices to possess or distribute CSAM. During the interview DACID obtained consent to search The DEVICE. DACID also obtained consent to search PV2

FERNANDEZ's Reddit account for photos, videos, emails, Reddit against degenerative subs chats, downloads, and search history.

16. On February 20, 2024, a DACID agent examined The DEVICE and found CSAM. Further examination of The DEVICE ceased pending authorization to examine the device further.

17. The DEVICE contained CSAM images including various videos of a minor female who appears to be between the ages 4-10 years old with brown hair, a stuff toy blanket, and a thin build. The minor female was seen positioned on her back on a bed with an adult male on top engaging in vaginal sex. The adult males face is not readily available. A second video included a minor male between the ages of 8-12 years old, brown/black short hair, fully undressed, thin in stature engaging in vaginal sex with a female between the age of 30-37 years old. The female had long brown/black hair, her stomach area was not excessively large, but also not flat, is seen laying on her back with her t-shirt on and pants off engaging in vaginal sex with the minor male.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, items that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

19. As further described in Attachment B, this application seeks permission to located not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the cell phone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the cell phone because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is

evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, it is sometimes necessary to establish that a particular thing is not present on a storage medium.

f. I know that an electronic device can be an instrumentality of the crime and also can be a storage medium for evidence of the crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was use; data that was sent or received; and other records that indicate the nature of the offense.

20. In addition to any electronic evidence described above, I am seeking authority to search for any items detailed in Attachment B.

21. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your Affiant is applying for would permit the examination of The DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

22. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, your Affiant submits there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. Based on all the above-listed facts and circumstances, your Affiant believes that probable cause exists for a search warrant authorizing the examination of The DEVICE, described in Attachment A, to seek the items described in Attachment B, which will constitute evidence and instrumentalities concerning violations of Title 18 of the United States Code Sections 2252 and 2252A (possession, receipt, and distribution of child pornography).

24. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States… that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

25. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

James D. Hawkins
Special Agent
Army Criminal Investigation Division

Subscribed and sworn to before me on the 12th day of March 2024

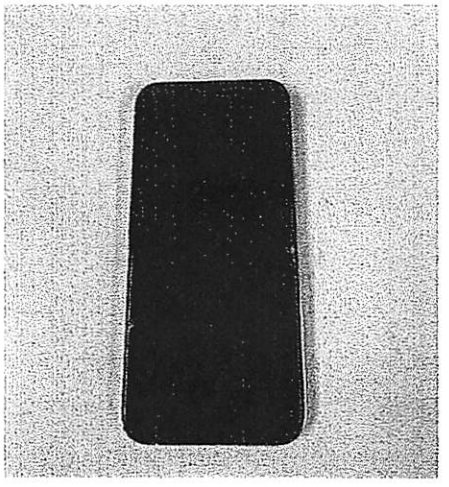
AMANDA MAXFIELD GREEN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

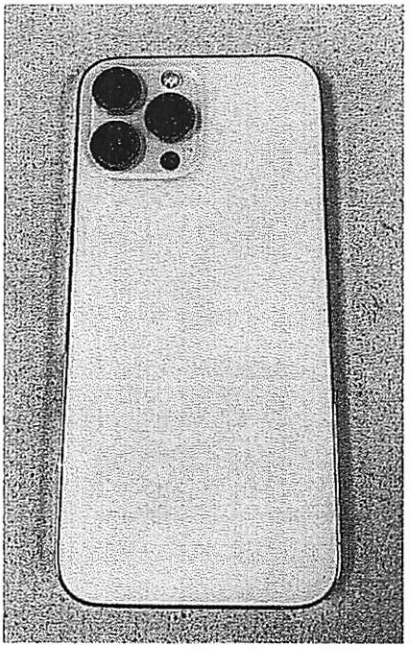
This warrant applies to the below listed mobile phone:

1. PV2 Kristian FERNANDEZ's Apple iPhone 13 Pro Max, serial number RQWHJXMTPH (hereafter "The DEVICE"), to include all files and folders contained within, held by DACID.

Front of The DEVICE



Back of The DEVICE



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. All electronically stored information on The DEVICE described in Attachment A that depict child pornography or communications or other records that show a violation of Title 18 of the United States Code Sections 2252 and 2252A (possession, receipt, and distribution of child pornography), including any electronic records or data that show the creation, transmission, possession, distribution, or receipt of child pornography, including, but not limited to:

   a) Images or visual depictions of child pornography.

   b) Any and all information, notes, documents, records, or correspondence, in any format or medium, pertaining to child pornography or sexual activity with or sexual interest in minors.

   c) Records relating to documentation or memorialization of the criminal offenses above, including voice memos, photographs, notes, memos, videos, emails, and other audio and video media, and all information and metadata attached thereto including device information, geotagging information, and information of the relevant dates related to the media.

   d) Records relating to the planning and execution of the criminal offense above, including Internet activity, including firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information.

   e) Application data, including but not limited to Facebook, Instagram, Snapchat, Twitter, Kik, Wickr, WhatsApp, Messenger, Youtube, Reddit, Telegram

relating to the criminal offenses above.

2. Evidence of user attribution showing who used or owned The DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved use names and passwords, documents, and browsing history.
3. All records and information related the geolocation of The DEVICE at a specific point in time.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form (such as digital image files; microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies)..

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, DACID may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.